National Infrastructure Protection Center
CyberNotes NIPC CyberNotes

Issue #1 *January 5, 1999*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at www.fbi/nipc/index.htm.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between December 10 and December 31, 1998. The table provides the operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site. Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified.

Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
3Com Network Management Card (NMC) for Total Control Hubs (TCHs)[1]	HARDWARE	Remote user can access remotely using a default account.	The adm account should be disabled, not deleted. If deleted, the account appears to reinstall on hardware reboot. Note that any hardware reboot over time will reactivate the account.	3Com default adm account on NMCs	Medium/ High	Default passwords available on Web sites and newsgroups.
3com HiPer[2]	HiPer ARCs running 4.1.11	Nestea Denial-of-Service (DOS) exploit script will cause card to fail and reboot.	Total Control NetServer card fixed problem but the HiPer ARC appears to have reintroduced the problem.	Nestea DOS	Medium	Exploit scripts posted to newsgroups and Web sites.
BreezeCOM[3] (SA 10, SA 40, AP 10)	HARDWARE	Local user can access adapter through default passwords.	No workaround available.	BreezeCOM default password	Low/ Medium	Default passwords available on Web sites and newsgroups.
Cisco IOS[4] 12.X, 11.3AA, and 11.3DB	Operating System	NMAP User Datagram Protocol (UDP) scans crashes routers running listed version of the software.	A tested workaround is to block incoming syslog traffic using the access list.	Cisco IOS Nmap crash	High	Exploit script (nmap) posted to newsgroups and Web sites. Hackers known to be using.
Embedded intelligent controllers or Programmed	OS –9	Internet Control Message Protocol (ICMP) redirect attacks leading to system	Workaround is to remove, where possible, these systems from the TCP/IP network.	Embedded intelligent controller ICMP shutdown	High (individual site risk is Low/	Current hacker tools will initiate this condition.

[1] Bugtraq, December 21, 1998.
[2] Bugtraq, December 21, 1998.
[3] Bugtraq, December 10, 1998.
[4] Bugtraq, December 22, 1998.

Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
logic Controllers (PLCs)[5]		shutdown or hanging.			Meduim)	
HP JetDirect[6]	JetDirect interface card	DOS attack against print services and printers.	Newer JetDirect cards are not affected.	JetDirect Denial of Service	Low	No scripts or exploits identified at time of publishing.
HP9000 series 700/800[7] 9.x to 11.X	Operating system (SNMP)	Remote user can gain root access using a buffer overflow (previous advisory issued).	Patches now available from Hewlett-Packard (HP).	SNMP buffer overflow	High	Exploit scripts posted to newsgroups and Web sites.
Iomega Zip Disk[8]		Unauthorized user can gain access to a password protected Zip disk.	Workaround is to place all passwordprotected disks in a locked container when not in use.	ZIP disk password removal	Low/ Medium	Unauthorized user must have physical access to the Zip disk that is protected.
Irix [9] 6.4 or higher	Fcagent daemon	DOS against FiberVault.	Patches are available at: http://www.sgi.com/Support/security/security.html	Fcagent DOS	Low	No scripts or exploits identified at time of publishing.
Irix[10] V 6.5	Operating system (inetd)	Nmap scan will cause inetd to fail if multiple server scans occur.	No workarounds known at time of publishing.	Nmap scanning	Medium	Exploit script (nmap) posted to newsgroups and Web sites. Hackers known to be using.
Linux[11]	Pluggable Authentication Modules (PAMs)	Local user can read and write to /etc/shadow and gain superuser privileges. This vulnerability exists for a limited time.	Patches available on some Linux software support sites. A temporary fix is to chmod –s /usr/bin/passwd.	Pam default exploit	Low/ Medium	No scripts or exploits identified at time of publishing.
Linux[12] (all versions)	WordPerfect 8	If a privileged user installs WordPerfect, root compromise is possible.	Set $TMPDIR before running the install script and do not run the install script as superuser or other highly privileged account.	WordPerfect 8 directory permission problem	High	No scripts identified at time of publishing. Explanation of exploit available in newsgroups.
Linux Red Hat [13] (lpr 0.31-1 or 0.33-1)	Lpd	DOS caused by remote user occurs if a remote user attempts to print to a printer server they do not have an account on.	No tested patches or workarounds available.	Linux Red Hat lpd remote user Denial of Service	Low/ Medium	Properly configured firewall will stop this attack from outside.
Microsoft[14]	Excel	Using the call function in Excel some executables can be run without the user's knowledge.	Patch is available at: http://offficeupdate.microsoft.com/downloaddetails/x197cfp.htm	Excel call function vulnerability (aka. Russian New Year exploitation)	Low/ Medium	No scripts identified at time of publishing.

[5] ISS Security Advisory, ICMP redirects against embedded controllers.

[6] ISS Security Advisory, HP Jetdirect TCP/IP problems.

[7] HP Daily Security Bulletin, HPSBUX9811-088 updated.

[8] Counterpane System's Ctypto-gram, December 15, 1998.

[9] Silicon Graphics Inc. Security Advisory, 19981201-01-PX.

[10] Bugtraq, December 22, 1998.

[11] Bugtraq, December 23, 1998.

[12] Bugtraq, December18, 1998.

[13] Bugtraq, December 18, 1998.

[14] Microsoft Security Bulletin (MS98-018).

Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Microsoft[15]	Internet Explorer	Malicious Web site can impersonate a legitimate Web site.	Patch is available at: http://www.microsoft.com/windows/ie/security/spoof.asp	Internet Explorer Frame Spoofing or Untrusted Scripted Paste	Low/ Medium	No scripts identified at time of publishing.
Microsoft Window NT[16]	Operating System Server 4	The network monitor process netmon.exe will fail when attempting to view a session request from a machine with a NetBIOS Scope Identifier of 190 or more characters.	No workarounds known at time of publishing.	Windows NetBIOS Scope ID problem	Low/ Medium	No scripts identified at time of publishing.
Microsoft Windows 98[17]	Operating System	Nmap scan will cause a critical error to develop (Blue Screen) and network connectivity is lost.	No workarounds known at time of publishing.	Nmap scanning	Medium	Exploit script (nmap) posted to newsgroups and Web sites. Hackers known to be using.
Yahoo – Multiple systems[18]	Yahoo pager	DOS by deactivating an identity.	No workarounds known at time of publishing.	Yahoo paper identity DOS	Medium	Exploit script posted to newsgroups.
NeXTStep[19] V3.3	Operating System	Nmap scan will cause the system to panic and reboot.	No workarounds known at time of publishing.	Nmap scanning	Medium	Exploit script (nmap) posted to newsgroups and Web sites. Hackers known to be using.
SCO UNIX OpenServer[20]	Operating system (calserver)	Remote user can gain root access using a buffer overflow.	No workarounds known at time of publishing.	Calserver	High	Exploit script posted to newsgroups and Web sites.
Sun Internet Mail Server (SIMS) 3.x[21]	SIMS	Remote user can read and write to the slapd.log file. This file has clear text passwords and uids of everyone checking mail.	No workarounds known at time of publishing.	SIMS slapd.log world read/write vulnerability	High	Limited Unix knowledge required to exploit this vulnerability. Hackers known to be exploiting this hole.
Sun Lightweight Directory Access Protocol (LDAP) Directory Services (SDS)[22] 1.x and 3.1	LDAP SDS	Remote user can read and write to the slapd.log file. This file has clear text passwords and uids of everyone checking mail.	No workarounds known at time of publishing.	slapd.log world read/write vulnerability	High	Limited Unix knowledge required to exploit this vulnerability. Hackers known to be exploiting this hole.
Sun Solaris[23] (multiple versions)	Operating system (inetd)	Nmap scan will cause inetd to fail if server scans occur.	No workarounds known at time of publishing.	Nmap scanning	Medium	Exploit script (nmap) posted to newsgroups and Web sites. Hackers known to be using.
Sun Solaris[24] 2.3 to 2.6	Operating system (Bind)	Remote user can gain root access using a	Patches available at: http://sunsolve.com/sunsolve/pubpa	Bind	High	Exploit scripts posted to

15 NTSHOP, December 23, 1998.
16 NTBugtraq, December 12, 1998.
17 SecureXpert labs Advisory SC-98.12.23-01.
18 Bugtraq, December 25, 1998.
19 SecureXpert Labs Advisory SC-98.12.23-01.
20 BugTraq, December 29, 1998.
21 Bugtraq, December 25, 1998.
22 Ibid.
23 SecureXpert Labs Advisory SC-98.12.23-01.
24 Sun Microsystems, Inc. Security Bulletin, #00180.

Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
		buffer overflow (previous advisory issued).	tches/patches.html			newsgroups and Web sites.
Sun Solaris[25] 2.4 to 2.6	Common Desktop Environment (CDE) dtmail	Remote user can execute programs with the privileges of mail or user reading mail.	Patches available at: http://sunsolve.com/sunsolve/pubpatches/patches.html.	Dtmail buffer overflows	High	No scripts or exploits identified at time of publishing.
Unix (many Berkeley Software Distributions [BSD] derived systems)[26] BSD/OS 3.1 FreeBSD prior to 2.2.8 FreeBSD 3.0 prior to 11/12/1998	Operating system (TCP/IP stack)	Remote user can cause a DOS condition in many implementations.	Patches available at: ftp://ftp.freebsd.org/pub/FreeBSD/CERT/patches/CA-98-13/patch	BSD TCP/IP stack weakness	Low/ Medium	Current hacker tools will initiate this condition.

*Risk is defined in the following manner:

High – A vulnerability that will allow an intruder to immediately gain privileged access (e.g., Sysadmin, root) to the system. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

Medium – Any vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

Low - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service attack. The reader should note that while the Denial-of-Service attack is deemed low from a threat potential, the frequency of this type of attack is very high. Denial-of-Service attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a "High" threat.

[25] Sun Microsystems, Inc. Security Bulletin, #00181.

[26] CERT Advisory CA-98.13.

Recent Exploit Scripts

The table below contains a representative sample of exploit scripts, identified between December 10 and December 31, 1998, listed by date of script, script name, script description, and testing conducted. Items listed in boldface (if any) are attack scripts for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches. During this time period, 50 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Testing Conducted
Dec 31, 1998	**Flushot.c**	**Denial-of-Service (DOS) C code that sends Central Processing Unit (CPU) usage to 100% on Windows 95/98 machines.**	
Dec 31, 1998	**Net-RawIP v0.03d**	**Perl module that manipulates raw ip packets and Ethernet headers.**	
Dec 30, 1998	**Net-RawIP v0.03c**	**Perl module that manipulates raw ip packets and Ethernet headers.**	
Dec 29, 1998	Aggressor PRO v1.0	Network vulnerability testing tool.	
Dec 29, 1998	Sco-calserver-bof.c	Exploit script in C code for the SCO Unix calserver buffer overflow.	
Dec 29, 1998	Sco-calserver-bof.sh	Exploit script in shell code for the SCO Unix calserver buffer overflow.	
Dec 29, 1998	Sbouncer.c	Bouncer that is used with wingate and socks proxies.	
Dec 29, 1998	Nmap v 2.02	Network scanning tool that has a variety of scanning modes, including stealth, Xmas, and Null stealth scans. Note: This tool is being used by hackers and may cause systems to become unstable.	
Dec 29, 1998	Lk2.pl	Perl script that scans for AFS file systems running Hesiod name servers checking for user directory permissions.	
Dec 28, 1998	**Net-RawIP v 0.03b**	**Perl module that manipulates raw ip packets and Ethernet headers.**	
Dec 28, 1998	Freebsd-mbuf-crash.c	DOS script which causes FreeBSD to fail.	
Dec 27, 1998	Pschack.c	Program that attempts to scavenge connections of an Internet Service Provide (ISP). Scavenging attempts to capture and use a connection that a user believes is closed. This is an effective method for hiding an attacker's identity.	
Dec 27, 1998	SDI-bnc.c	Buffer overflow exploit script for bnc.	
Dec 27, 1998	THC-SCAN v2.0	War dialer with many auto-identification features.	
Dec 27, 1998	Vanity.c	BNC remote buffer overflow for Linux x86 (without the stack-non-exec patch). Works on versions below 2.4.4.	
Dec 24, 1998	Kcmsex.c	Exploit script for the Solaris i386 /usr/openwin/bin/kcms_configure hole.	
Dec 22, 1998	Bootpd-bb.tar.gz	Bootp exploit against Debian Linux 1.3 and 2.0.	
Dec 22, 1998	Cheops v0.58	Tool for network scanning and discovery of operating system. Note: The author of the tool has posted warnings that the tool has the potential of being misused and there have been indications that hackers are currently using this tool.	
Dec 22, 1998	Lamescan v1.4	Port scanner that will perform random scans and multithread scans. It will also scan host names as they are typed on stdin, ansi, and identd lookups. It will send a string "user XXXX" in an effort to defeat automated port scan detectors.	
Dec 22, 1998	Mdmrst.c	Implements the +++ATH0 modem bug and is capable of spoofing.	
Dec 22, 1998	Miffo-check.c	Port scanner.	
Dec 22, 1998	Rely v1.0	Forwards traffic for a port to any other host and port designated by the user.	
Dec 22, 1998	Resetter.c	DOS tool that attempts to reset all connections of a network segment by sending spoofed RST and ICMP UNREACHABLE packets.	
Dec 22, 1998	Snort v0.96	Fairly portable packet (Solaris, Linux, and FreeBSD) sniffer.	
Dec 22, 1998	Stuffit.c	Modified ping flood that contains an illegal character for Point-to-Point Protocol (PPP).	
Dec 22, 1998	Tgk-log v2.1	Designed to record contents of packets as they pass through an ipmasq gateway.	
Dec 22, 1998	Usr-totalswitch.txt	Backdoor passwords for all versions of US Robotics' Totalswitch.	

Date of Script (Reverse Chronological Order)	Script Name	Script Description	Testing Conducted
Dec 21, 1998	Nessus WIP 122198	Security audit tool that checks for over 150 known holes. (Trojan horse versions found.)	
Dec 19, 1998	dcc-hijack.c	Hijacking tool for the DCC chat/send/receive sessions of many Internet Relay Chat (IRC) clients.	
Dec 19, 1998	**Exscan v0.2**	**Port scanner with a strobe scanning capability.**	
Dec 19, 1998	**Valueclick-cgi.txt**	**Exploit for Valueclick online advertising agency Web interface that captures usernames/passwords.**	
Dec 18, 1998	Bootp_exploit.c	Remote buffer overflow (bootpd) exploit code for many Unix systems.	
Dec 18, 1998	PortScanner v1.2	A port scanner with strobe scanning capability.	
Dec 18, 1998	Squid_connect.tar.gz	Exploit on squid proxy server used to hide an intruder's identity.	
Dec 18, 1998	Suck.c	Sample sniffer code.	
Dec 18, 1998	Tellme.tar.gz	Script that retrieves netbios name over the network.	
Dec 18, 1998	Udplstn.tar.gz	Daemon that hooks User Datagram Protocol (UDP) ports and then records all incoming packets.	
Dec 18, 1998	Webspf.pl	Program that spoofs referer page and will bypass most reference checking.	
Dec 17, 1998	Nmap v2.01	Network scanning tool that has a variety of scanning modes, including stealth, Xmas, and Null stealth scans. Note: This tool is being used by hackers and may cause systems to become unstable.	
Dec 17, 1998	Scancd.pl.	New port scanner written in Perl.	
Dec 17, 1998	Syn.pl	Script designed to detect stealth scans performed by nmap.	
Dec 14, 1998	Cheops v0.57	See description above.	
Dec 14, 1998	Game.exe	Trojan horse program with the NetBus exploit attached.	
Dec 14, 1998	Hping v0.66	Ping-based program for network mapping. Note: A number of hacker sites are recommending that this tool be used.	
Dec 14, 1998	Kkill.c	Opens hundreds of connections to a single host in a DOS effort.	
Dec 14, 1998	Nmap v2.00	See description above.	
Dec 14, 1998	Sxploit.sh	Tool that scans local system for a number of old vulnerabilities and then attempts to exploit vulnerabilities discovered.	
Dec 13, 1998	Lportfuck.c	DOS attack script.	
Dec 13, 1998	Nessus WIP 121398	See description above.	
Dec 11, 1998	Murderkill Deluxe v2.0	Package of many DOS scripts that automate the launching of multiple attacks.	

Note: A number of scripts have been updated during this two-week period (e.g., Nmap, Nessus WIP, Cheops). The hacker community is constantly improving the tools they use.

Trends

1. Several hackers appear to be using coordinated scans and probes from different sites.
2. More phreaker tools are appearing on hacker Web sites.
3. Scanning for IMAP and POP continues.
4. A significant increase in reports of NetBus and BackOrifice scanning is occurring.
5. A set of scripts has appeared that identifies hosts running Linux, responds on TCP port 111, and then attempts exploitation of the mountd vulnerability.
6. A new TCP port scan method has appeared that uses spoofed addresses of "zero traffic" hosts to identify open ports.
7. A rapid increase is noted in the use of hacker/Phreaker tools developed for the PalmPilot.

Viruses

Remote Explorer - In the last few weeks, a virus known as Remote Explorer has received a great deal of press. Network Associates Inc. (NAI) issued warnings to the Microsoft Windows computing community. This virus was first discovered on December 17, 1998, at an MCI WorldCom facility. This virus compresses executables and encrypts some file types, hampering recovery of data. Detection of the current version can be accomplished by going to the control panel and checking services for a file titled "Remote Explorer." If this file is discovered, then the machine is infected. The virus is unique in that it is the first virus discovered that uses network services to allow it to spread. Once on a network server, the virus spread rapidly to workstations and other trusted servers. Most major anti-virus vendors have upgraded their products to detect the virus and some have the capability to remove the virus and recover any affected files. Anti-virus vendors recommend that their users update the anti-virus packages on a regular basis (every two weeks).

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). You are encouraged to share this publication with colleagues in the information and infrastructure protection field.